Release Notes for Cisco NCS 540 Series Routers, Cisco IOS XR Release 6.6.25

Revised: July 22, 2022

Network Convergence System 540 Series Routers

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

System Requirements

Cisco IOS XR Release 6.6.25 contains all features released in Cisco IOS XR Release 6.6.1.

Cisco IOS XR Release 6.6.25 contains all features released in Cisco IOS XR Release 6.6.1. Release 6.6.1 is limited availability (LA) release. For more information on IOS XR Release 6.6.1, see *Release Notes for Cisco NCS 540 Series Routers, Release 6.6.1*

Release 6.6.25 Packages

This table lists the Cisco IOS XR Software feature set matrix (packages) with associated filenames.

Table 1: Release 6.6.25 Packages for Cisco NCS 540 Series Router

Composite Package		
Feature Set	**Filename**	**Description**
Cisco IOS XR IP Unicast Routing Core Bundle	ncs540-mini-x.iso-r6.6.25	Contains base image contents that includes: • Host operating system • System Admin boot image • IOS XR boot image • BGP packages
Individually-Installable Optional Packages		
Feature Set	**Filename**	**Description**
Cisco IOS XR Manageability Package	ncs540-mgbl-1.0.0.0-r6625.x86_64.rpm	Extensible Markup Language (XML) Parser, Telemetry, Netconf, gRPC and HTTP server packages.

Cisco IOS XR MPLS Package	ncs540-mpls-1.0.0.0-r6625.x86_64.rpm ncs540-mpls-te-rsvp-1.0.0.0-r661.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.
Cisco IOS XR Security Package	ncs540-k9sec-1.0.0.0-r6625.x86_64.rpm	Support for Encryption, Decryption, Secure Shell (SSH), Secure Socket Layer (SSL), and Public-key infrastructure (PKI)
Cisco IOS XR ISIS package	ncs540-isis-1.0.0.0-r6625.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs540-ospf-1.0.0.0-r6625.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs540-li-1.0.0.0-r6625.x86_64.rpm	Includes LI software images
Multicast Package	ncs540-mcast-1.0.0.0-r6625.x86_64.rpm	Support Multicast

Determine Software Version

To verfiy the software version running on the router, use the **show version** command in the EXEC mode.

```
RP/0/RP0/CPU0:Router #show version
Cisco IOS XR Software, Version 6.6.25
Copyright (c) 2013-2019 by Cisco Systems, Inc.

Build Information:
 Built By     : <username>
 Built On     : Wed May 29 07:03:08 PDT 2019
 Built Host   : iox-lnx-028
 Workspace    : /auto/srcarchive13/prod/6.6.25/ncs540/ws
 Version      : 6.6.25
 Location     : /opt/cisco/XR/packages/

cisco NCS-540 () processor
System uptime is 46 minutes

RP/0/RP0/CPU0:Router# show install active
Node 0/RP0/CPU0 [RP]
  Boot Partition: xr_lv147
  Active Packages: 9
        ncs540-xr-6.6.25 version=6.6.25 [Boot image]
        ncs540-mgbl-1.0.0.0-r6625
        ncs540-mpls-1.0.0.0-r6625
        ncs540-ospf-1.0.0.0-r6625
        ncs540-mpls-te-rsvp-1.0.0.0-r6625
        ncs540-mcast-1.0.0.0-r6625
        ncs540-isis-1.0.0.0-r6625
        ncs540-li-1.0.0.0-r6625
        ncs540-k9sec-1.0.0.0-r6625

Node 0/0/CPU0 [LC]
  Boot Partition: xr_lcp_lv148
  Active Packages: 9
        ncs540-xr-6.6.25 version=6.6.25 [Boot image]
        ncs540-mgbl-1.0.0.0-r6625
        ncs540-mpls-1.0.0.0-r6625
        ncs540-ospf-1.0.0.0-r6625
        ncs540-mpls-te-rsvp-1.0.0.0-r6625
        ncs540-mcast-1.0.0.0-r6625
        ncs540-isis-1.0.0.0-r6625
        ncs540-li-1.0.0.0-r6625
        ncs540-k9sec-1.0.0.0-r6625
```

Determine Firmware Support

Use the **show fpd package** command in Admin mode to view the hardware components with their current FPD version and status.

```
RP/0/RP0/CPU0:Router# show fpd package

=============================== ================================================
                                        Field Programmable Device Package
                                ================================================
                                               Req     SW      Min Req   Min Req
Card Type            FPD Description           Reload  Ver     SW Ver  Board Ver
=================== ========================== ====== ======= ======== =========
--------------------------------------------------------------------------------
N540-24Z8Q2C-M       Bootloader(A)              YES     1.11    1.11    0.0
                     CPU-IOFPGA(A)              YES     0.03    0.03    0.0
                     MB-IOFPGA(A)               YES     0.18    0.18    0.0
                     MB-MIFPGA                  YES     0.04    0.04    0.0
                     SATA(A)                    NO      5.00    5.00    0.0
--------------------------------------------------------------------------------
N540-ACC-SYS         Bootloader(A)              YES     1.11    1.11    0.0
                     CPU-IOFPGA(A)              YES     0.03    0.03    0.0
                     MB-IOFPGA(A)               YES     0.18    0.18    0.0
                     MB-MIFPGA                  YES     0.04    0.04    0.0
                     SATA(A)                    NO      5.00    5.00    0.0
--------------------------------------------------------------------------------
N540-X-24Z8Q2C-M     Bootloader(A)              YES     1.11    1.11    0.0
                     CPU-IOFPGA(A)              YES     0.03    0.03    0.0
                     MB-IOFPGA(A)               YES     0.18    0.18    0.0
                     MB-MIFPGA                  YES     0.04    0.04    0.0
                     SATA(A)                    NO      5.00    5.00    0.0
--------------------------------------------------------------------------------
N540X-ACC-SYS        Bootloader(A)              YES     1.11    1.11    0.0
                     CPU-IOFPGA(A)              YES     0.03    0.03    0.0
                     MB-IOFPGA(A)               YES     0.18    0.18    0.0
                     MB-MIFPGA                  YES     0.04    0.04    0.0
                     SATA(A)                    NO      5.00    5.00    0.0
```

Use the **show hw-module fpd** command in EXEC mode to view the hardware components with their current FPD version and status. The status of the hardware must be CURRENT; Running and Programed version must be the same.

```
RP/0/RP0/CPU0:Router# show hw-module fpd
Wed May 29 17:31:51.715 UTC
                                                               FPD Versions
                                                               =================
Location   Card type        HWver FPD device       ATR Status   Running Programd
------------------------------------------------------------------------------
0/RP0     N540-24Z8Q2C-M    1.0   MB-MIFPGA            CURRENT    0.04    0.04
0/RP0     N540-24Z8Q2C-M    1.0   Bootloader           CURRENT    1.11    1.11
0/RP0     N540-24Z8Q2C-M    1.0   CPU-IOFPGA           CURRENT    0.03    0.03
0/RP0     N540-24Z8Q2C-M    1.0   MB-IOFPGA            CURRENT    0.18    0.18
```

Supported Software Features for N540-24Z8Q2C-SYS, N540X-ACC-SYS, and N540-ACC-SYS

Following are the features supported on Cisco N540-24Z8Q2C-SYS, N540X-ACC-SYS, and N540-ACC-SYS variants.

ACL Support for PCEP Connection

PCE protocol (PCEP) (RFC5440) is a client-server model running over TCP/IP, where the server (PCE) opens a port and the clients (PCC) initiate connections. After the peers establish a TCP connection, they create a PCE session on top of it.

The ACL Support for PCEP Connection feature provides a way to protect a PCE server using an Access Control List (ACL) to restrict the PCC peers at the time the TCP connection is created based on the source address of client. When a client initiates the TCP connection, the ACL is referenced, and the client source address is compared. The ACL can either permit or deny the address and the TCP connection will proceed or not.

For more information about ACLs, see the Implementing Access Lists and Prefix Lists chapter in the IP Addresses and Services Configuration Guide.

For more information about the ACL Support for PCEP Connection feature, see the Configure Segment Routing Path Computation Element chapter in the .

Bridge Domain and BVI Scale

The number of bridge domains depends on the number of attachment circuits (ACs) per bridge domain and if the Bridge-Group Virtual Interface (BVI) is configured or not. In Release 6.6.25, only 750 BDs are supported.

Ethernet Flow Point Visibility

The Ethernet flow point (EFP) visibility feature enables you to configure multiple VLANs in the same bridge-domain.

The EFP service instance is a logical interface that connects a bridge domain to a physical port or to an EtherChannel group. A VLAN tag identifies the EFP.

Prior to this release, only one EFP is allowed per bridge-domain. With the EFP visibility feature, you can configure a maximum of 600 EFPs per bridge-domain.

For more information refer the chapter *Configure Virtual LANs in Layer 2 VPNs* in the , *Release 6.6.x*

Explicit Congestion Notification (ECN) Bit Marking

The Expilicit Congestion Notification (ECN) feature is an extension to WRED (Weighted Random Early Detection). This feature will mark packets instead of dropping them when the average queue length exceeds a specific threshold value. When configured, ECN helps routers and end hosts to understand that the network is congested and slow down sending packets.

For more information on this feature, see the .

Flow Label Support for EVPN VPWS

The Flow Label support for EVPN VPWS feature enables provider (P) routers to use a flow-based load balancing to forward traffic between the provider edge (PE) devices. Flow-Aware Transport (FAT) pseudowires (PW) over an MPLS packet switched network is used for load-balancing traffic across BGP-signaled pseudowires for an EVPN virtual private wire service (VPWS).

For more information on this feature, see the *EVPN Virtual Private Wire Service (VPWS)* chapter in the *, IOS XR Release 6.6.x.*

Ingress Short-Pipe

Usually, DSCP and precedence-based classifications are supported in QoS traffic only when there is no MPLS label in the packet. Using the ingress short-pipe feature, however, you can classify a packet that contains one MPLS label using the type-of-service (ToS) field of the IPv4 or IPv6 header.

With the ingress short-pipe feature, you get increased visibility into traffic packets. Plus, the feature also removes the limitation of classifying MPLS packets that come into IPv4 or IPv6 networks.

To know more about the selective egress policy-based queue mapping feature, see the . To see the command reference details, see *match mpls disposition class-map child_pipe* in *Modular QoS Command Reference for Cisco NCS 5500 Series and Cisco NCS 540 Series Routers*.

IPv6 Multicast for Multiple Sources

Before this release IPv6 multicast support was limited to a single source for each multicast group. However, when multiple sources were involved then it resulted in duplicating multicast flows of multiple sources to all interested receivers.

LDP-Based VPLS and VPWS FAT Pseudowire

The LDP-based VPLS and VPWS FAT Pseudowire feature enable provider (P) routers to use a flow-based load balancing to forward traffic between the provider edge (PE) devices. Flow-Aware Transport (FAT) of pseudowires (PW) over an MPLS packet switched network is used for load-balancing traffic across LDP-signaled pseudowires for Virtual Private LAN Services (VPLS) and Virtual PrivateWire Service (VPWS).

For more information on this feature, see the *Configure Multipoint Layer 2 Services* chapter in the *, IOS XR Release 6.6.x.*

LDP over Segment Routing Policy

The LDP over Segment Routing Policy feature enables an LDP-targeted adjacency over Segment Routing (SR) policy between two routers. This feature extends the existing MPLS LDP address family neighbor configuration to specify an SR policy as the targeted end-point.

For more information about the LDP over Segment Routing Policy feature, see the Configure SR-TE Policies chapter in the .

MAC Address Withdrawal

The MAC Address Withdrawal feature provides faster convergence by removing MAC addresses that are dynamically learned. This feature uses Label Distribution Protocol (LDP)-based MAC address withdrawal message. A MAC list Type Length Value (TLV) is part of the MAC address withdrawal message.

This feature also supports optimization of MAC address withdrawal. The optimization allows PEs to retain the MAC addresses that are learned from the CE devices over the access side. Only MAC addresses that are learned from peer PEs are flushed out. This avoids unnecessary MAC flushing toward AC side and ensures better utilization of bandwidth and resources.

For more information on this feature, see the *Configure Multipoint Layer 2 Services* chapter in the *, IOS XR Release 6.6.x.*

Static Route Traffic-Steering using SRTE Policy

Earlier, you could associate Segment Routing Label Switched Paths (SR-LSP) with a static route. The Static Route Traffic-Steering using SRTE Policy feature adds support to specify a Segment Routing (SR) policy as an interface type when configuring static routes for MPLS and IPv6 data planes.

For more information about the Static Route Traffic-Steering using SRTE Policy feature, see the Configure SR-TE Policies chapter in the .

Three-level Hierarchical QoS

The Three-level Hierarchical QoS (H-QoS) feature enables enforcement of class/service, group/ ethernet flow point (EFP), and port level SLAs.

As earlier, you can apply the regular two-level egress H-QoS policies on the sub-interfaces to achieve class and EFP SLAs at child and parent levels. In addition, with this feature, you can apply a port shaper policy on the main interface to achieve an aggregated port level SLA in a 1+2 H-QoS model.

The advantage of three-level H-QoS is that the parent shaper on the sub-interfaces is allowed to oversubscribe, thus enabling best effort sharing of the aggregate port shaper at the third level.

To know more about the three-level Hierarchical QoS feature, its sample configuration, and other information, see the .

New Hardware Features Introduced in IOS XR Release 6.6.25

There are no new hardware features introduced in this release.

Supported Optics

The following optics are supported on the Cisco NCS 540 Series router in this release:

- GLC-BX40-D-I
- GLC-BX40-DA-I
- GLC-BX40-U-I
- GLC-BX80-DI
- GLC-BX80-UI
- SFP-10G-BX-D-I
- SFP-10G-BXU-I
- SFP-10G-BX40-DI
- SFP-10G-BX40-UI
- GLC-LX-SM-RGD
- SFP-10/25G-LR-S
- GLC-T-RGD

Supported MIBs

The Cisco NCS 5500 MIB support list is also applicable to the Series Routers. For the list of supported MIBs, see the Cisco NCS5500 MIB Support List.

Restrictions and Limitations on the Cisco NCS 540 Series Router

The following restrictions are applicable only to Cisco N540-24Z8Q2C-SYS, N540X-ACC-SYS, and N540-ACC-SYS variants.

- In the Cisco IOS XR Release 7.0.1, the Packet IO feature is not supported on bundle interfaces.
- The **show inventory** and the **show diagnostic** commands do not display the fan serial number.

- The interface ports 0/0/0/24 to 0/0/0/31 do not support 1G Copper SFPs.
- Remove the speed settings on the 1G Copper optics when 10M/100M is configured and replaced with 1G SFP optics.
- The **hw-module profile mfib statistics** command is not supported.

Caveats

This section describes open and resolved severity 1 and 2 caveats and select severity 3 caveats:

- The "Open Caveats" sections list open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.
- The "Resolved Caveats" sections list caveats resolved in a specific release, but open in previous releases.

The bug IDs are sorted alphanumerically.

Note The Caveats section includes the bug ID and a short description of the bug. For details on the symptoms, conditions, and workaround for a specific caveat you must use the Bug Search Tool.

Cisco IOS XR Caveats Release 6.6.25

Caveat ID Number	**Descriptiom**
CSCvo76722	Ethernet internal Loopback drops 256 byte packets

Note SFP-10/25G-LR-S will work only in 25G mode and not supported on 10G mode.

Upgrading Cisco IOS XR Software

Cisco IOS XR Software is installed and activated from modular packages, allowing specific features or software patches to be installed, upgraded, or downgraded without affecting unrelated processes. Software packages can be upgraded or downgraded on all supported card types, or on a single card (node).

The upgrade document (NCS540_Upgrade_MOP_6.6.25.pdf) is available along with the software images.

Production Software Maintenance Updates (SMUs)

A production SMU is a SMU that is formally requested, developed, tested, and released. Production SMUs are intended for use in a live network environment and are formally supported by the Cisco TAC and the relevant development teams. Software bugs identified through software recommendations or Bug Search Tools are not a basis for production SMU requests.

For information on production SMU types, refer the *Production SMU Types* section of the *IOS XR Software Maintenance Updates (SMUs)* guide.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.